



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/623,488	10/30/2000	Feng Bao	P19949	7274
7055	7590	09/01/2006	EXAMINER	
GREENBLUM & BERNSTEIN, P.L.C. 1950 ROLAND CLARKE PLACE RESTON, VA 20191				PARTHASARATHY, PRAMILA
ART UNIT		PAPER NUMBER		
				2136

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Supplemental
Notice of Allowability

Application No.	Applicant(s)	
09/623,488	BAO ET AL.	
Examiner	Art Unit	
Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS. This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to 7/26/2006.
2. The allowed claim(s) is/are 8-18; Renumbered as 1-11.
3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

NASSER MOAZZAMI
PRIMARY EXAMINER

M
7/31/06

U.S. Patent and Trademark Office
PTOL-37 (Rev. 7-05)

Notice of Allowability

Part of Paper No./Mail Date 20060728

Specification

The abstract of the disclosure is objected to because of undue length. Correction is required. See MPEP § 608.01(b).

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

ABSTRACT

"A Method of Exchanging Digital Data"

A method of exchanging digital signatures (sign_A, sign_B) between a first and a second party (A, B) includes the first party encrypting sign_A and generating an authentication certificate (Cert_A), the Cert_A authenticating that the encrypted signature (C_TA) is an encryption of the signature of the first party. The first party (A) sends the C_TA and the Cert_A to the second party (B) which verifies that the C_TA is an encryption of the sign_A of the first party (A), and if the verification is positive, the second party (B) sends its sign_B to the first party (A) which, in turn, verifies that the sign_B is the digital signature of the second party (B), and if the verification is positive, the first party sends its unencrypted signature (sign_A) to the second party. The second

Art Unit: 2136

party (B) verifies that the sign_A is the first party's digital signature, and accepts the sign_A if the verification is positive. If the verification is negative, the second party (B) sends the encrypted C_TA and sign_B to an independent third party (T). The third party (T) decrypts the (C_TA) of the first party (A) to obtain the first party's sign_A, and verifies that the sign_A, sign_B are verified as the digital signatures of the first and second parties (A, B), the third party (T) sends sign_A to the second party (B) and sign_B to the first party (A).